# Correlating Risk Events And Process Trends To Improve Reliability

Bryan Singer
Kenexis Security Corporation
Columbus, Ohio
bryan.singer@kenexis.com

**Abstract:** Cost justifying security improvements persists as a challenge to improving Industrial Control Systems (ICS) Security. Low rates of reported incidents and vulnerabilities for ICS as compared to similar electronic systems in IT leaves many to question whether or not cyber security for ICS is truly a challenge. The quest for Return on Investment (ROI) and business justification for improved security controls persists as an impediment to reducing risk despite increasing awareness, vulnerability discovery and reporting, and attack trends. This paper explores another potential vector to justify security expenditures through the identification, measurement, and improvement of process trends that are affected by improved security controls.

**Keywords:** Risk Management, Loss of View, Loss of Control, ICS Network Performance, Overall Equipment Effectiveness,

## 1 Introduction

In the absence of clear risk data, reducing risk is a nebulous goal; however, reducing uncertainty is a much more attainable goal. Identifying specific and measurable events, and then correlating these events to process trend data, such as maintenance costs, machine efficiencies, quality, and other data, affords an opportunity to not only improve operations, but also reduce cyber security risk. Many security controls are of multiple benefit, such as improving network reliability and reducing manual change control errors.

This paper explores methods to attain specific and measurable network and process performance related events and methods for correlating process trends to these events. Through the analysis, detection and trending of anomalous process events and association against process Key Performance Indicator (KPI) trends, security measures can thus be justified through directly improving overall process efficiency and reliability.

### 1.1 Audience

The audience for this paper is control engineers, safety engineers, operations managers, information technology personnel and managers with responsibility for industrial networking, industrial cyber security researchers, or similar parties. This paper assumes a basic familiarity with TCP/IP networking, basic control theory, and general familiarity

with the systems, communications, design and management of typical process architectures.

## 1.2 Terminology

Where appropriate, the document explains in context terminology that is not commonly understood. Table 1 below is as a reference for frequently used acronyms.

| Acronym | Expansion |
|---|---|
| **ALE** | Annualized Loss Expectancy |
| **ARO** | Annualized Rate of Occurrence |
| **DCS** | Distributed Control Systems |
| **ERP** | Enterprise Resource Planning |
| **EV** | Exposure Value |
| **HMI** | Human Machine Interface |
| **ICS** | Industrial Control Systems |
| **KPI** | Key Performance Indicators |
| **LIMS** | Laboratory Information Management Systems |
| **MES** | Manufacturing Enterprise Systems |
| **OEE** | Overall Equipment Effectiveness |
| **PLC** | Programmable Logic Controller |
| **RF** | Reduction Factor |
| **SCADA** | Supervisory Control and Data Acquisition |
| **SIS** | Safety Instrumented Systems |
| **SLE** | Singularized Loss Expectancy |
| **SPC** | Statistical Process Control |
| **VFD** | Variable Frequency Drives |

*Table 1 – Acronym Expansion*

# 2 Challenges of Risk Management for ICS Networks

This section presents a simplified ROI study for network and security expenditures, and explores the various weaknesses of this approach.

## 2.1 Simplified Risk Analysis and ROI Example

The following example was adapted from a summation of multiple projects in which a detailed cost benefit and ROI was required to justify spending. For the purposes of this example, the following tenets are made:

- This example summarizes cost, benefit and risk on an average per plant unit of measurement.

- The costs are summarized across an entire global enterprise environment on a standard measurement of currency for 100 total plants.
- Singularized Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), Annualized Loss Expectancy (ALE), Reduction Factor (RF), and Residual Risk are all summarized into aggregate categories of failures.
- A RF is applied based upon observation of previous trends and failures as well as qualitative judgments based upon an agreed to definition and categorization of security events (such as viruses, unauthorized logic changes, excessive user permissions and related failures, etc.).

Given the complex nature of significant or catastrophic failures, the more significant the event, the higher the cost, and also the less likely it is to be mitigated. As an example, consider the 1994 Texaco Refinery Explosion and the 2005 BP Texas City Explosion. These instances reveal that while they occur infrequently, the more complex the failure, the more difficult it is to prevent.

### 2.1.1 High Level Risk Analysis

Using information from interviews and other evaluations, Table 2 – Common High Level Risk Analysis represents categories of failures, with SLE, ARO, and RF. The extended ALE is computed based on 100 total plants, and the SLE, ARO, and ALE are computed on an average per site basis.

| Event | SLE | ARO | ALE | Extended ALE | RF | Residual Risk |
|---|---|---|---|---|---|---|
| Minor | $50,000 | 10 | $500,000 | $50,000,000 | 65% | $17,500,000 |
| Moderate | $250,000 | 3 | $750,000 | $75,000,000 | 55% | $33,750,000 |
| Significant | $1,000,000 | 0.2 | $200,000 | $20,000,000 | 25% | $15,000,000 |
| Catastrophic | $20,000,000 | 0.01 | $200,000 | $20,000,000 | 5% | $19,000,000 |
| | | | $1,650,000 | $165,000,000 | ($79,750,000) | $85,250,000 |

*Table 2 – Common High Level Risk Analysis*

### 2.1.2 High Level Cost Analysis

Table 3 shows some typical costs for a set of security and network improvements, including firewall, router and switch upgrades, and the associated labor and infrastructure costs.

| Cost Item | Cost Per Site |
|---|---|
| Firewall | $75,000 |
| Routers and Switches | $125,000 |
| Cabling and Infrastructure | $25,000 |
| Labor | $72,000 |
| Cost Per Site | $297,000 |
| Extended Cost | $29,700,000 |

*Table 3 – Sample Cost Sheet (Simplified)*

### 2.1.3 Computations for ROI and Common Pitfalls

Given a cost of $29.7M and a totalized risk reduction of $79.75M, a simple ROI based on risk reduction alone computes to 52.76%. While Table 2 and Table 3 provide only summary information, implying a cursory qualitative risk assessment, experiential data gathered over nearly 100 security assessments shows that these trend towards a central mean regardless of the level of quantitative precision. One reason for this is that all risk management at some level is qualitative, relegated to "best estimate" generated by consensus of parties involved.

ROI numbers such as the above tend to be unbelievable. A typical ROI to justify capital expenditures is in the range of 30-33%, with strict qualification on the measurement criteria to clearly achieve the stated benefit. The security ROI is frequently less tangible due to absence of clear performance measurements and therefore less believable than other process variables. Consequently, the security ROI frequently fails the justification criteria. A number of common contributing factors that complicate security ROI calculations include the following:

1. Risk management teams fail to properly define, qualify or track security events.
2. A lack of operator and management visibility into process floor failures occurs through insufficient observation, reporting, tracking or trending of relevant events.
3. Insufficient incident, vulnerability and intelligence data in industry limits effectiveness and precision of risk ARO calculations.
4. Despite even the best information, security expenditures are almost always viewed as a cost with no tangible benefit by management.

Association of process failures tends to favor easily observed factors such as machine failures, application failures or other causal factors given the physical nature of a process and the basic interaction with the process by operators. Practitioners in ICS networking and security have long since discussed the need for proper infrastructure.

One study conducted by Rockwell Automation in 2004 found that as high as 65% of process application failures had exacerbating or primary causal failures in network infrastructure performance. As such, there is a prima facie argument here that if so many failures in a process have network components, how do we go about measuring and improving processes through reducing these failures?

## 2.2 Cyber Fragility

Cyber fragility is a useful concept in understanding the role of network related failures. A 2010 paper by Ralph Langer defines cyber fragility as:

> "Cyber fragility is the deficient ability of an automated process to withstand variations of "normal", data related operating conditions during the process' lifetime, even though the variation is inside the limits of typical operating environment characteristics, and analysis shows that such variation could and should well have been anticipated. Failures are often of a "surprising" nature, and not directly attributed to an otherwise abnormal event. Nevertheless, network related failures are indeed deterministic, can be measured, and subsequently reduced. Failures often occur despite operations well within accepted and "normal" operation parameters, leaving operations and maintenance staff wondering what exactly went wrong." [1]

The author has analyzed several hundred process failures resulting in extended process inefficiencies, stoppages, or even catastrophic and dangerous failures. Conclusions and observations show a nearly universal presence of network related causal factors. These conclusions warrant a deeper inspection of network traffic, and indicate that the reduction of these incidents will provide sufficient cost / benefit for both network and security expenditures.

# 3 Limitations of Traditional Network Analysis for ICS Networks

In a typical information systems network, a CDA model of Core, Distribution, and Access is used to integrate communications. Communications are characterized by client to server, server to client, and offsite communications such as web browsing, business to business systems, email, and other office or personal traffic. While many organizations consider their communications as "time critical" (sometimes inaccurately referred to as "real time") delays of several hundred milliseconds to several seconds are nearly always considered acceptable.

While some level of communications is expected between clients at the Access layers in CDA architecture, the bulk of observed communications involve local client-server or offsite communications. This model is rarely found in a typical ICS network, where communications are highly meshed, frequently geographically dispersed, and time critical as well as crossing multiple OSI Layer 1 media types.

## 3.1 Performance Management in a Traditional Business Network

To assure reliable and efficient network communications, the primary points of analysis on the network include inspection of OSI Layer 1 (Physical) and OSI Layer 2 (Data Link) communications at the switches and routers comprising the basis of the communications architecture. Layer 1 and Layer 2 inspection is common place through tools such as SNMP, switch statistics, and utilizing sniffers on SPAN or monitor ports on managed switches.

While tools like Netflow offer some OSI Layer 3 (Network) inspection, the typical office IT environment is adequately supported by Layer 1 and Layer 2 inspection only. Assuring performance at these layers is provided through verifying the electrical integrity of the media, switches, and routers and checking for the availability of the source and destinations workstations through simple Layer 3 queries such as ICMP Echo Request/Reply (aka ping). Figure 1 – Network Service versus Applications Communication represents the typical layer 1 and 2 inspection.

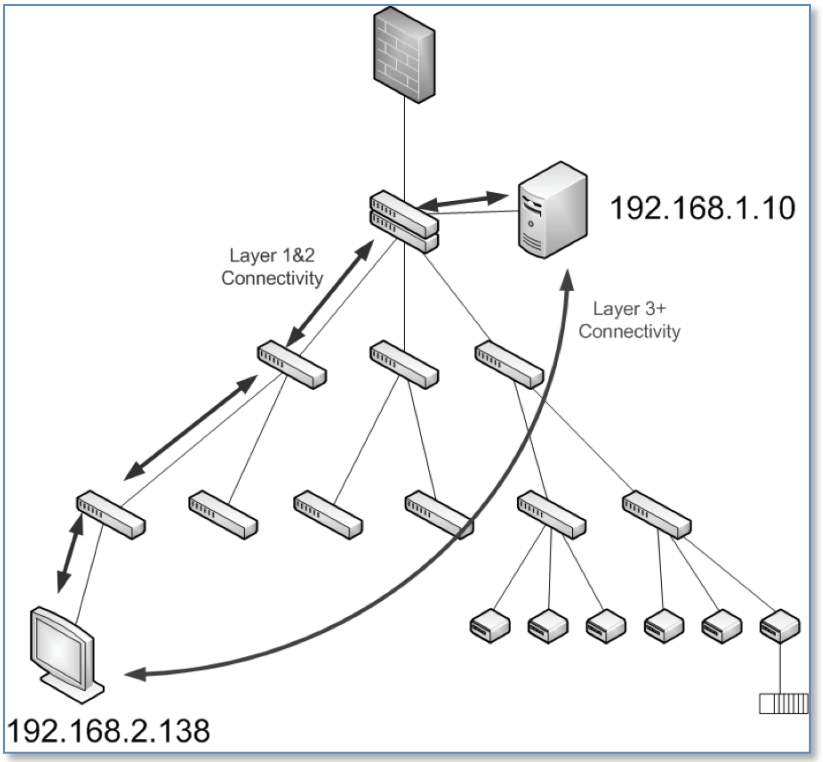


*Figure 1 – Network Service versus Applications Communication*

# 4 ICS Networking Challenges

## 4.1 Failure Modes for ICS Networks

ICS networks connect control assets, and the communication between these assets is critical to ensure availability of the process. The following four categories of failures are useful in analyzing ICS network and process events. During significant or catastrophic failure incidents, there is a natural progression through each of these levels. Once operators lose an accurate view of the system state, they may not be aware of impending failures, or may take inappropriate action based upon available feedback. The primary exception to this would be that MoV typically only occurs in intentional events.

- Loss of View (LoV): Loss of accurate view of system assets creates the risk of operators taking inappropriate or harmful actions due to the inaccurate knowledge of system state. LoV typically occurs through denial of service, loss of communications, slow network response, or similar conditions that prevent HMI's or operator workstations receiving an accurate view of the current system state.
- Manipulation of View (MoV): Harmful actions are possible in intentional scenarios where misdirection is used to encourage inappropriate operator response. Some operator errors that result in issues such as improper screen updates could be considered MoV, but primarily MoV is an intentional incident.
- Denial of Control (DoC): Through unintentional or intentional denial of service, deny operators the ability to interact with critical control points in a process. Unintentional causes include operator accidents, hardware failures, network failures, improper network capacity, or similar failures. DoC can occur in ICS networks when operator instructions are prevented from reaching the destination control system through various network faults.
- Loss of Control (LoC): Denial of Control represents conditions where operators can interact with the system, but workarounds, alternate communications paths, or other opportunities still exist for operators to intervene in possible system impacts. Loss of Control implies a sustained loss or race / runaway conditions in which operators cannot take alternate action before the full system impact is realized. Loss of Control is typically a process condition in which a failure is imminent and unavoidable.

These failure modes are useful in analyzing previous known failures, or in modeling ways in which ICS network or process failures could occur due to ICS network anomalies. For example, reviewing LoV or MoV opportunities in a system, security analysts and control engineers can determine the potential for an inaccurate or manipulated view of the current system state could lead operators to take potentially harmful actions. A useful exercise is to consider the 2005 BP Texas City Refinery Explosion in which there were a number of operator actions taken that exacerbated the catastrophic failure – actions which were inappropriate for the actual system state and based on inaccurate view.

## 4.2 Communications Challenges in ICS Networks

An ICS network is comprised of multiple communicating endpoints across various levels of the ICS network, and possibly separated by large geographic spaces requiring extensive transformations from physical network media to wireless, satellite, cellular, or other communications. While such complexities can be found in the typical office environment, the ICS network is often unique. A limited time critical window exists in which to complete a successful process instruction; otherwise, nuisance trips or fail-safe shutdown protocols are likely to occur. During this window, all operator instructions, performance indicators, feedback loops, alarms, and any other required actions must function correctly in the proper sequence and timing. While response times at layers 0 and 1 of the Purdue Reference Model can be as short as 10-20ms, typical times are between 300-750ms to maintain operations of these time critical functions. Control and feedback instructions at layers 2 and above can range from milliseconds to minutes depending upon the process type and architecture.

Exceeding these times can lead to fail-safes, process failures, product rejects, control loop failures or other undesirable conditions. To the operator, these may often appear as unexplained failures, or are easily attributed to other process conditions such as poor raw materials, application failures, improperly tuned control logic or maintenance failures. Rarely is the network is observed as primary causal factor of the failure.

## 4.3 Communications Needs for ICS Networks

Figure 2 below represents a typical round trip communication for a single process control command issued from an operator workstation.

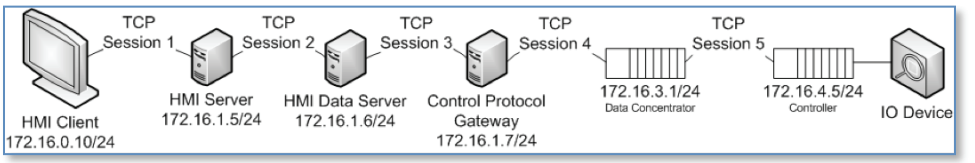


*Figure 2 – Typical Process Control Architecture Dataflow*

Multiple sessions are constructed between the HMI to the various servers, gateways, data concentrators, controllers and eventually to the actual devices such as an actuator, valve, etc. In all actuality, the above model is extremely limited in representing the live operational state of the system. There is often control loop logic at the controller and at various points in this architecture that is ongoing independent of operator instructions. The communications are further by independent systems such as Safety Instrumented Systems (SIS), and data repository connections to historians, MES, LIMS, ERP, SPC, or other components found in nearly every process architecture.

Figure 3 – TCP Sessions in a Typical Single Process Control Command shows the same process control type command represented across a typical ICS network architecture. It is entirely likely that at many as 19 independent TCP sessions may be required to

execute even a single process instruction. Such instructions involve disparate systems across various routers, VLAN's or switches. And given the time critical nature of these communications, any latency, misconfiguration or other interruptions can manifest as a failure, missed instructions, improper system feedback or otherwise.

Any failure to update a critical component in time can result in an inaccurate view of the current system state that can lead to process failures, inappropriate operator actions based on faulty information, or in severe cases safety or catastrophic failures.

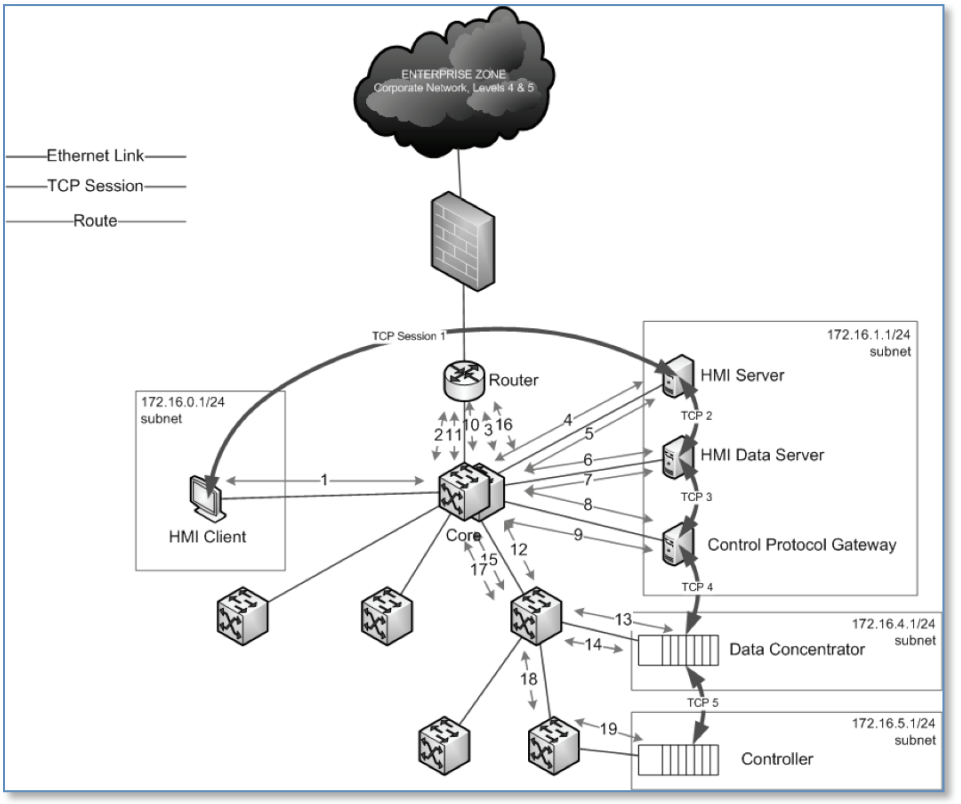


*Figure 3 – TCP Sessions in a Typical Single Process Control Command*

## 4.4 Vulnerabilities in ICS Networks

Since 2007, Wurldtech Security Technologies has been conducting an ongoing study named Delphi, which is an effort to aggregate discovered vulnerabilities in several dozen DCS, SIS and other ICS components. While this study still represents only a subset of the total population of ICS systems worldwide, it nevertheless provides some key insight for system designers when considering the deployment of an ICS network. Their data

further is supported by the author's experiential observations across several hundred network and security assessments spanning nearly 15 years. [2]

Figure 4 – Distribution of Vulnerabilities by Protocol Type illustrates Delphi findings regarding vulnerabilities found based on protocol type, and that common networking errors in traditional protocols are a frequent causal factors in ICS network failures.

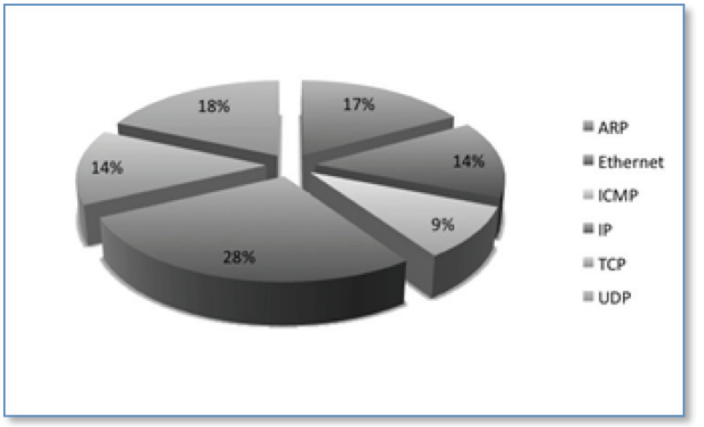


*Figure 4 – Distribution of Vulnerabilities by Protocol Type*

Figure 5 – Importance of Rate in Vulnerability Exploitation expands on the above by illustrating that most of the ICS network vulnerabilities found are rate dependent, meaning that at higher traffic rates the failures manifest.

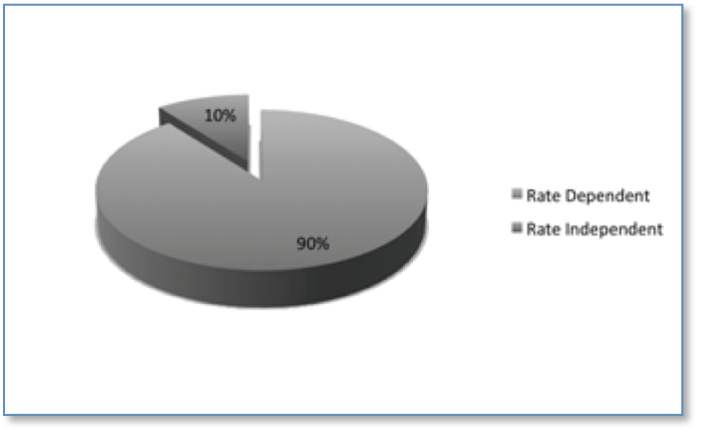


*Figure 5 – Importance of Rate in Vulnerability Exploitation*

For system designers and ICS network managers, these results reinforce the need for careful design, planning and maintenance of an ICS network.

## 4.5 Misalignment of Analysis and Management of ICS Network Performance

A common misperception when analyzing ICS networks is to assume that sufficient bandwidth is a primary indicator of adequate network performance. Experiential observations find that while most ICS networks operate at less than 2% utilization, process faults frequently result from ICS network issues. Consider Figure 6 – Traffic I/O Graph and Figure 7 – Network Utilization Example from a recent project involving a steel mill comprised of four process lines. The point of observation was the plant to IT network gateway.

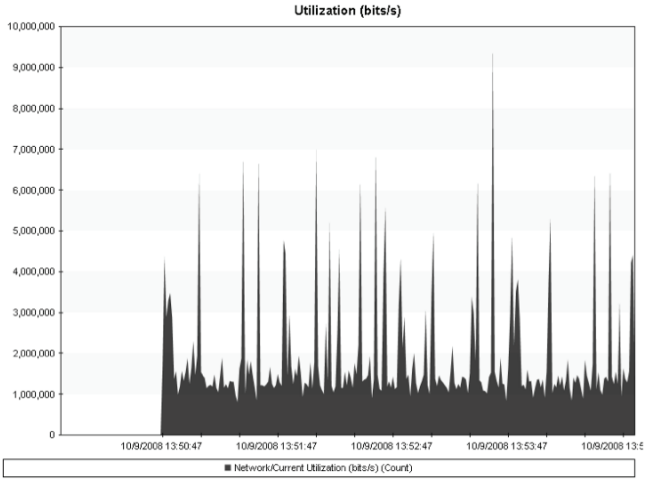


*Figure 6 - Traffic I/O Graph*

| Network | Value |
|---|---|
| Total Bytes | 56737970 |
| Total Packets | 288084 |
| Total Broadcast | 201952 |
| Total Multicast | 5621718 |
| Average Utilization (percent) | 0.190 |
| Average Utilization (bits/s) | 1,900,388.867 |
| Current Utilization (percent) | 0.136 |
| Current Utilization (bits/s) | 1,355,312.000 |
| Max Utilization (percent) | 0.957 |
| Max Utilization (bits/s) | 9,573,608.000 |

*Figure 7 – Network Utilization Example*

In this example, process failures, application update delays, and nuisance trips frequently occurred due to network related faults. The faults occurred despite utilization peaking at less than 1%. Considering that this network peaks far below typical switch backplanes speeds of 32 or 64 Gbps, previous analyses concluded that the network was not a causal factor in the process failures. Several considerable problems were observed at lower levels of the ICS network due to aged OSI layer 2 network switches and hubs and improper management of broadcast domains.

### 4.6 Conclusions for ICS Networking

The above clearly illustrates the disparate communication needs between typical business or office networks and ICS networks. Latency is observed as the number one disrupter of ICS networks, given the stated assumptions of this paper. Latency manifests as a number of easily observed network conditions:

- TCP errors (fast retransmissions, retransmissions, duplicate acks, etc.)
- TCP receive window size shrinkage
- Excessive round trip time (different from TTL)
- TTL (Time to Live)

Latency nearly always is introduced as a result of various discrepancies across the seven OSI layers including poor design, bad media, improper configuration or other factors.

## 5 An Alternative Method for Risk Management

Before anything can be measured or improved for an ICS network or security environment, greater clarification is needed:

- Definition of security "events"
- Dismissal or acceptance criteria of security or network events for risk reduction measurement
- Agreement on how to differentiate between intentional and unintentional events – the author preferring to not make the distinction as it is not the cause but the effect that generates loss
- Gathering of past data to analyze previous failures or recognizing additional measurement capabilities that may be needed.

The criteria above progress quickly from a largely undefined risk definition, to a much more precise definition in which a distinction is made based upon the certainty of the event. This provides the opportunity for the security professional to utilize more effective tools - namely, the reduction of risk through two distinct actions:

1. Reduction in Certain Events: Identification of measurable events that can be systematically reduced and subsequently associated to a clear measure of improvement.

2. Reduction in Uncertainty: The reduction of overall uncertainty and risk in the system through ancillary effects by addressing measurable events, and by gaining through measurement and improvement over time. [3]

## 5.1 Technique for Measuring ICS Network and Security Performance

The author, as well as many other industry specialists in ICS networks, has adopted practices for specific measurement throughout an ICS network at various access points. This is accomplished through aggregating multiple network observations across various collection points into an overall picture of network health. This picture is balanced against production trends to target and prioritize specific improvements to assure process reliability. What makes an ICS network and security specialist unique in his or her practice comes from a three-step process:

1. Measure OSI Layer 1 and 2 performance at the main points of connectivity between IT and the process. This is accomplished through gathering of SNMP data, switch statistics, usage of network analyzers and other tools. As previously indicated, this is where most traditional IT network analysis techniques cease.
2. Coupling knowledge of industrial protocols and applications, inspect Layer 3 performance and higher layers to understand issues such as potential or actual failures of process control equipment. This involves the construction of filters and rules in network sniffers or similar inspection tools to observe data at the transactional level with an understanding of how process control devices communicate. Observations, such as in the Wurldtech report and other experiential data, provide an additional level of visibility as to how, why and when process equipment can fail.
3. Cost determination and cost/benefit calculation is driven by this last layer of analysis in which the analysts reviews previous failure data, or inspects trends and events in process intelligence applications, such as historians, to identify both previous failure data and to determine the impact of network infrastructure improvements against process performance.

## 5.2 Measuring Process Performance

In a modern plant infrastructure, hardly a single action goes unnoticed. Information systems, technologies and manual processes work together to analyze run time and post production performance to maximize efficiency, assure safe operation and improve performance. These include alarm and event workstations, HMI's, light panels, cameras, operators, paper travelers, historians, SPC, and MES. Any measurable action or event can be identified and traced in an operating process. With sufficient correlation and analysis, measurements can be associated to costs and performance. While traditional monitoring focuses primarily on the physical nature of the process, this paper demonstrates that there is sufficient opportunity for additional inspection and correlation.

Measurements can be generally lumped into two categories of KPI, which are used at various points of analysis ranging across process equipment, lines, sites and the enterprise:

- Measured Value KPI: These are simple values such as number of cases, temperature, pressure,or other single point values. They are meant to provide immediate feedback but have little additional value.
- Calculated KPI: These can be considered as either simple or complex. Simple involves summation, average or other calculation of two or more Measured Value KPI's, such as cases per hour comparing time and a case count. Complex involves multiple simple calculated KPI's such as planned versus unplanned downtime, trends of cases per hour over a period of time or number of different sites, etc.

KPI's are stored in information systems such as historians and MES, with the bulk of any calculation being handled by the application itself, and presented in various formats such as dashboards, line graphs or finite values.

## 5.3 Opportunities for Comparison of ICS Network Events and Process KPI's

In the ICS network arena, Measured Value KPI's are those such as packet counts, and simple Calculated KPI's are measurements such as utilization. These are of little value initially in that they are gathered from the network devices and traditionally stored separately from production KPI's. Further, correlation of simple values to process trends is normally insufficient to properly identify network related causal factors that impact process efficiency. As such, it is the complex Calculated KPI's that offer the most opportunity for comparative analysis and reduction. One such KPI that has been used by the author extensively is Overall Equipment Effectiveness (OEE). OEE is often utilized throughout a process architecture in many discrete industries, and is commonly found at least at the machine level in process industries.

### 5.3.1 OEE as a Case Example

OEE is a measurement of the maximum theoretical output for a given process, and a delineation of causal factors that prevent the achievement of this theoretical maximum. While different industry verticals or local corporate culture adopt KPI's suitable for measuring their particular environment, this paper focuses on OEE. OEE is useful as it is a complex Calculated KPI based on commonly measured and understood process performance measurements. OEE is frequently used to determine production bottlenecks, to identify machines that should be targeted for upgrade, and to perform comparative analysis against similar processes or plants. This OEE analysis data is then used to target and subsequently measure specific performance improvements.

The basic OEE measurement is the product of three Calculated KPI's: Availability x Performance x Quality.

- Availability is the measure of uptime of the process: how much time was it scheduled to be up versus how much time it actually was up
- Performance is the theoretical maximum output in a specified unit of measure (UoM), both provided by the equipment supplier or design engineer, for a machine or a line
- Quality is the ratio of first pass acceptable units in the stated UoM that were produced against the number of units that were rejected, reclaimed, or reworked

Table 4 provides an OEE computational example.

| Measure | Value |
|---|---|
| Availability | 90% |
| Performance | 95% |
| Quality | 99.9% |

*Table 4 – OEE Computational Example*

The resulting OEE is .9 * .95 * .999 which is .854 or 85.4%.

Determining what is an acceptable OEE is largely dependent on corporate culture and other practices such as Six Sigma. Most organizations begin with a period of measurement first, then comparison across sites, and then systematic improvement. Commonly, the monetary value of a single percentage point increase or decrease in OEE is well known to the organization.

### 5.3.2 Typical Causal Factors behind OEE Losses

Table 5 from http://www.oee.com shows their summation of the "Six Big Losses" that impact OEE. [4]

| Six Big Losses | OEE Factor | Visual OEE™ |
|---|---|---|
| Breakdowns | *Availability* | • Availability<br>• Down Time (cumulative and event)<br>• Real-time production mode indication<br>• Reason Code tracking and analysis<br>• Statistics and metrics are real-time automated<br>• Operators can focus on getting equipment running |
| Setup and Adjustments | *Availability* | • Setup Time (cumulative and event)<br>• Set goals for Setup Time reduction programs |
| Small Stops | *Performance* | • Performance<br>• Average Cycle Time<br>• Small Stops (occurrences and time)<br>• Configurable Small Stop Threshold<br>• Cycle Time Trace records every cycle<br>• Identify when and how time is lost to Small Stops |
| Reduced Speed | *Performance* | • Reduced Speed (occurrences and time)<br>• Configurable Reduced Speed Threshold<br>• Cycle Time Trace records every cycle<br>• Identify Reduced Speed patterns |
| Startup Rejects | *Quality* | • Reject Pieces (during Startup)<br>• Percent Reject Pieces (during Startup) |
| Production Rejects | *Quality* | • Quality<br>• Reject Pieces (during Production)<br>• Percent Reject Pieces (during Production) |

*Table 5 – OEE "Six Big" Losses*

By inspecting the causal factors that contribute to these losses, the author observes that utilizing these ICS network analysis techniques provides effective tools to identify and mitigate ICS network related faults that contribute to process inefficiencies. Measurement and subsequent mitigation of these faults is thus an effective vehicle to justify network and security expenditures and is far more effective than standard risk analysis alone.

# 6 Automating Methods of Collection and Comparison

The techniques described herein have been applied on a case by case basis manually over many site assessments and are now being automated. Accepting that these trends can be effectively measured and correlated, the following are the key components to enable this process:

- Determination of ICS Network Events to Monitor – This set leverages items previously discussed as causal factors in ICS network failures. They largely do not distinguish between intentional or unintentional events, as the observed network anomaly is generally the same.
- Measurement and Recording of ICS Network Events – This is accomplished by gathering data through network sniffers attached to active taps or through active monitor / SPAN ports on switches, and by analyzing data with a rules based engine such as SNORT, trends and graphs, or traffic capture filters. It is important to note that for this to be effective, the traffic must be captured in transit between control components and not just on the core switches.
- Correlation against Process Data – This is accomplished by a rules based engine where data mining techniques are utilized to correlate the rate of occurrence of network events and process efficiencies.

## 6.1 Assuring Effective Measurement and Recording of ICS Network Events

There are a number of events that can falsely indicate network anomalies if not carefully analyzed. These events could occur during shift change operations, weekly or monthly updates, or other such periodic but infrequent events, as seen in Figure 8.

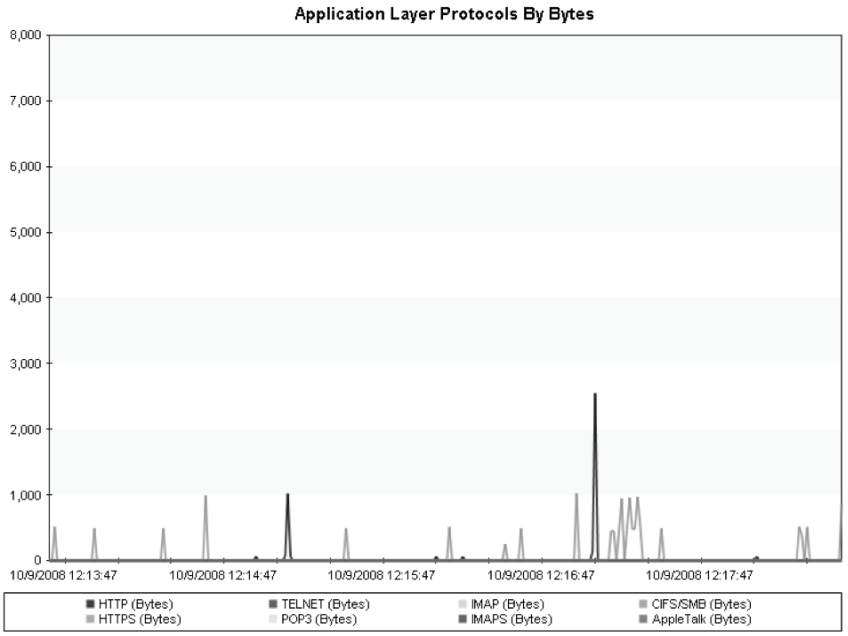


*Figure 8 – Example of ICS Network Capture*

The spike on the right in Figure 8 may be interpreted as an anomalous event. This may or may not be so; the only way to be certain is to normalize trends over time using techniques borrowed from Digital Sound Processing (DSP), line graphs, or other time based analysis over a greater delta of time, as in Figure 9 – Example of an I/O Graph Over Time.

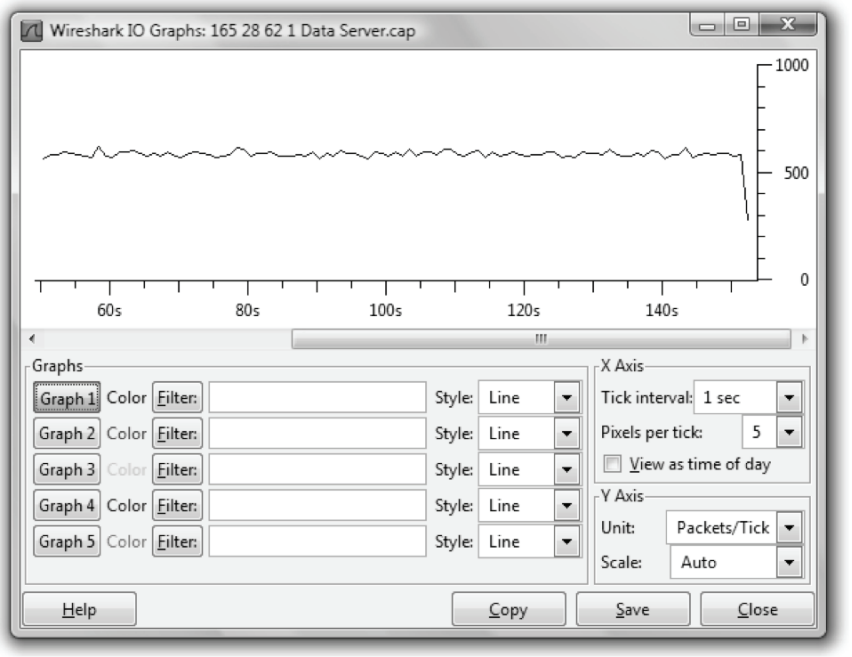


*Figure 9 – Example of an I/O Graph Over Time*

## 6.2 Effective Correlation to Process Trends

Effective correlation is accomplished by borrowing from SPC disciplines which determine sustained and average traffic over time. Gates are established for a given time domain which use mean computation to establish both High-Low (H-L) and High-High (H-H) states. Instances that exceed H-L or H-H states are subsequently compared to process trends, as in Figure 10 – SPC Applied to ICS Analysis.

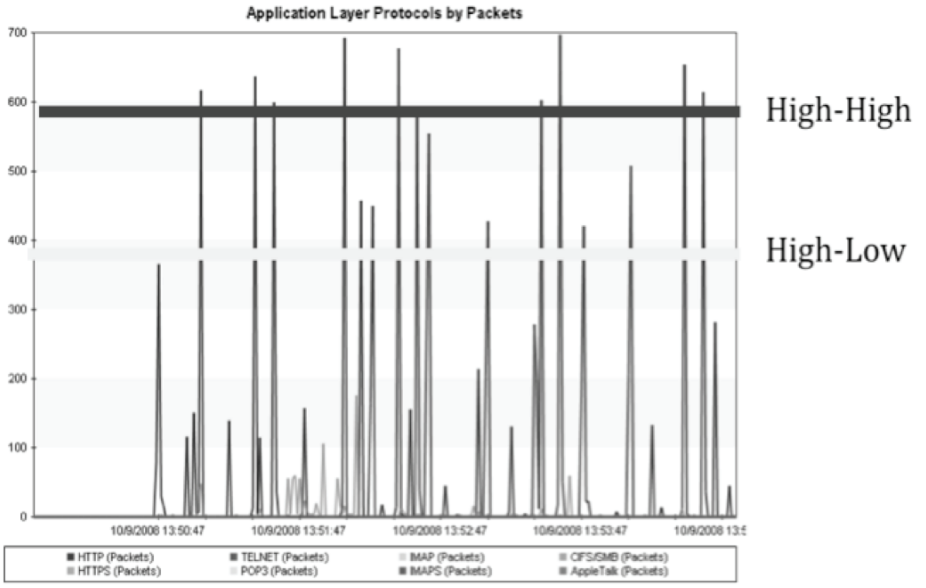


*Figure 10 – SPC Applied to ICS Analysis*

These counts are applied to gain understanding of impacts against calculated KPI's such as OEE. Most often, these causal factors impact the Performance or Availability components of OEE, but a limited measure of improvement of Quality has been observed.

# 7 Case Study

These techniques were applied to a large process industries customer and adapted for the following example. A known per point OEE increase / decrease value was provided by their financial controllership at $12,000 per percentage point, per line – as shown in Table 6.

| | Availability | Quality | Performance | OEE | |
|---|---|---|---|---|---|
| Pre | 96 | 97.5 | 92.33 | 86.42 | |
| Plan | 97.1 | 97.8 | 94.3 | 89.55 | |
| Actual | 97.08 | 97.72 | 94.01 | 89.18 | |
| | | | | 2.76 | $99,474.77 |

*Table 6 – OEE Example*

For a single plant with an average of three process lines, a 2.76% actual increase in OEE resulted in improvements valued at almost $100,000 per plant. With an average cost per plant of $297,000, an ROI in excess of 33% was noted. The pre-improvement values

were observed at existing levels prior to network analysis. Analysis was conducted with two numbers computed for post-improvement. One number was for the planned increase, and then the actual number was recorded a number of months after analysis.

# 8 Additional Benefits of Collecting and Analyzing Data with this Model

This paper outlines a process for collecting information to justify security expenditures, but suggests this model be utilized on a permanent basis. There are several reasons for this:

- Network traffic trends change over time with addition of new hardware, software, failures or process changes. This collection capability online will enable early detection of degrading performance issues that could impact future network reliability.
- Used as an online system and possibly integrated further with security trending tools and vulnerability detection, this model becomes an online early warning system that exceeds the capabilities of many rule based IDS systems to date. While behaving similarly to a heuristics based network intrusion detection system (NIDS), additional value is gained through the correlation against process tends.
- Through proper adaptation of collection techniques and storage of data, this system could be further adapted and utilized in a forensics capability.
- With the increase in trends for centralized location and streamlining of key support staff, this model could be highly effective in the determination, analysis and support of live systems without impacting production operations. Currently, supporting live ICS network failures remotely often requires several days of collection and analysis that the described system could reduce to hours.

# 9 Summary

This paper has inspected various mechanisms used today in ROI and benefit determination for ICS network and security improvements. This was accomplished through both discussion of various weaknesses and their impact in limiting support of security expenditures as well as exploring techniques currently in use to provide a greater integration between the currently disparate ICS network design and monitoring and process improvement initiatives. While a number of complexities beyond the scope of this limited paper exist, it is suggested and supported that the required tools and techniques needed fully exist today. These tools and techniques provide an enhanced ability to not only justify network and security expenditures, but also to improve the reliability, resilience and performance of industrial processes against ICS network and security threats.

**About the Author** – Bryan Singer is a Principal Investigator with Kenexis Security Corporation and Co-chairman of ISA-99 Industrial Automation and Control Systems Security standard. He began his professional career with the US Military focusing on issues such as physical, systems, network security and force protection. Since that time, he has spent significant time in cyber security projects focusing on risk analysis, vulnerability testing, penetration testing, risk mitigation strategies, and enterprise architecture and design including technical and policy based countermeasures and remediation strategies. Mr. Singer holds the CISSP and CISM certifications.

## References:

[1] Langner, R., Beyond Risk: Fundamentals of Robust Industrial Automation and Control Networks, 2010.

[2] Kube, D. N., Delphi at a Glimpse, Wurldtech Security Technologies, 2009.

[3] Hubbard, D. W., How to Measure Anything: Finding the Value of Intangibles in Business, John Wiley & Sons, Inc., 2007.

[4] Industries, V., Fast Guide to OEE, Retrieved Dec 15, 2009 from http://www.oee.com: http://www.oee.com/pdf/fast-guide-to-oee.pdf, 2008.